諸外国のサイバーセキュリティ政策について

資料5－1

	米国	EU	英国	日本
人材育成	Federal Cybersecurity Workforce Strategy（2016, Executive Office of the President） ➢ 人材のニーズを特定 ➢ 教育・訓練による人材補強 ➢ 多様な人材採用の促進 ➢ キャリアパスを構築し、高度なスキルを有する人材の維持・促進	The Directive on Security of Network and Information Systems （2016, European Commission） ➢ EU加盟国に対し、ネットワーク及び情報システムのセキュリティに関する国家戦略を定め、その中で、教育・普及啓発・人材育成に関する施策を含めることを要求	National Cyber Security Strategy 2016-2021(2016, Cabinet Office） ➢ 官民問わずセキュリティ人材の不足を解消するため、英国におけるセキュリティ人材の育成を柱のひとつとする。	サイバーセキュリティ人材育成総合強化方針(2016, 戦略本部） ➢ 民間分野、政府双方について、セキュリティ人材育成のための方針を策定 ➢ セキュリティ対策は費用ではなく、投資であるべきとの認識の下、橋渡し人材の育成を推進 サイバーセキュリティ人材育成プログラム(2017, 戦略本部）
重要インフラ防御（情報共有）	Cybersecurity Information Sharing Act（2015, U.S. House Committee on Homeland Security） ➢ サイバー脅威情報の官民共有の手続きの整備 ➢ 民間主体等について、情報共有に伴う法的責任を免除 ＜参考：重要インフラ16分野＞ 化学、商業施設、通信、重要製造業、ダム、防衛産業基盤、緊急対応サービス、エネルギー、金融、食料・農業、政府施設、ヘルスケア・公衆衛生、情報技術、原子炉・核物質・核廃棄物、輸送システム、水・排水システム	The Directive on Security of Network and Information Systems （2016, European Commission） ➢ 加盟国は、重要なサービス提供事業者において深刻なインシデントが発生した場合には、当該事業者が遅滞なく監督官庁への通知を行うための措置を講じる。 ＜参考：重要インフラ7分野＞ エネルギー、交通・輸送、銀行、金融、医療、水、デジタルサービス	Investigatory Powers Act（2016, Parliament of the United Kingdom） ➢ プライバシーに関する一般的義務規定の新設 ➢ コミュニケーションデータの取得・保存、特定令状やバルク令状の取り扱いについて規定 ・2016年に設立されたNCSC（国家サイバーセキュリティセンター）が主体となって、インシデント情報等の共有を実施 ＜参考：重要インフラ13分野＞ 化学、民間核施設、通信、防衛、緊急対応サービス、エネルギー、金融、食料、政府、健康、宇宙、交通、水	重要インフラの情報セキュリティ対策に係る第4次行動計画(2017, 戦略本部） ➢ 重要インフラサービスを、安全かつ持続的に提供できるよう、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進 ➢ オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。 ＜参考：重要インフラ13分野＞ 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油
IoTセキュリティ	Strategic Principles for Securing the IoT(2016, DHS） ➢ IoTセキュリティの課題解決に資する原則を記載 ・セキュリティ・バイ・デザイン ・セキュリティアップデート及び脆弱性管理 ・実績に基づくセキュリティプラクティスの構築 ・潜在的影響に応じたセキュリティ方策の優先順位づけ ・IoTの透明性の促進 ・慎重かつ熟慮したネットワークへの接続	Securing Europe’s IoT Devices and Services(2015, ENISA） ➢ 各分野における専門技術・ノウハウの展開 ➢ セキュリティのグッドプラクティスの促進 ➢ ステークホルダーの関与	National Cyber Security Strategy 2016-2021(2016, Cabinet Office） ➢ サイバーセキュリティ分野の科学技術への一層投資について言及され、考慮すべき重要分野の1つとしてIoTを挙げている。 The launch of the National Cyber Security Centre(2017, NCSC） ➢ IoTは、新しい機会を創出するものである一方、多くの新しい課題も存在すると言及	安全なIoTシステムのためのセキュリティに関する一般的枠組(2016, 戦略本部） ➢ 安全なIoTシステムが具備すべき一般要求事項としてのセキュリティ要件の基本的要素を明らかにしたもの。 IoTセキュリティガイドラインver1.0(2016, 総務省、経産省、IoT推進コンソーシアム） ➢ 「機器メーカ、サービス提供者などを対象にした5つの指針」及び「一般利用者を対象にしたルール」を分野横断的に定めたもの。

※NISC及び各関係機関の公表資料等を元に総務省が作成